USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 08/02/2022

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVID DE MEDICIS, *on behalf of himself and all others similarly situated*,

Plaintiff,

-against-

ALLY BANK and ALLY FINANCIAL, INC.,

Defendants.

No. 21 Civ. 6799 (NSR)
OPINION & ORDER

NELSON S. ROMÁN, United States District Judge:

This putative class action alleges that Defendants Ally Bank and Ally Financial, Inc. (collectively, "Defendants") negligently disclosed their customers' account usernames, passwords, and other private information to unnamed third parties through a coding error in Defendants' website portal (the "Coding Error"). (Compl. ¶¶ 1–11, ECF No. 5.) Plaintiff David De Medicis, on behalf of himself and on all others similarly situated, brings this action against Defendants asserting claims for negligence, negligence *per se*, breach of implied contract, violations of the Virginia Personal Information Breach Notification Act, and injunctive/declaratory relief under the Declaratory Judgment Act. (*Id.* ¶¶ 60–99.) Presently pending before the Court is Defendants' motion to dismiss Plaintiff's Complaint under Federal Rules of Civil Procedure 12(b)(1) and (6). (ECF No. 18.) For the following reasons, the Court GRANTS Defendants' motion to dismiss.

## BACKGROUND

### I. Factual Background

The following facts are derived from the Complaint, which are taken as true and constructed in the light most favorable to Plaintiff for the purposes of this motion. The following

facts are also derived from Defendants' proffered extrinsic evidence purportedly revealing the existence of factual problems in the assertion of jurisdiction.[1]

Plaintiff, a Virginia resident, maintains checking, savings, and securities accounts with Defendants, which are a digital financial-services company and its wholly owned subsidiary. (Compl. ¶¶ 12–14.)

On April 12, 2021, during a routine website update, Defendants learned of the Coding Error, which affected certain query strings that transmit information after a customer entered a username and password to access an online account with Defendants. (Compl. ¶¶ 22, 24; Hall Decl. ¶ 3, ECF No. 20.) These query strings—which send information across Defendants' platform to allow customers to access their online accounts—usually do not contain any personally identifiable information. (Hall Decl. ¶¶ 4–5.) The Coding Error, however, resulted in certain query strings that contained usernames and passwords (embedded within the string of code) being sent to a limited group of known entities with which Defendants have ongoing contractual and business relationships. (*Id.* ¶ 6.) For example, a query string with a customer's username and password (both redacted) looked like this:

> https://www.ally.com,/,/,/?hdmjavascriptdata=&allysf-login-v1-account=aaos&allysf-login-v1-username-78e30d704ccce8ccc7b8539f0144cb09=[redacted]&allysf-login-v1-password-78e30d704ccce8ccc7b8539f0144cb09=[redacted]

(*Id.* ¶ 9.) The Coding Error only occurred in limited circumstances where the user attempted to log in before the page had fully loaded—that is, when the user was using software to automatically

[1] As the Court will explain more fully below, "a defendant is permitted to make a fact-based Rule 12(b)(1) motion, proffering evidence beyond the Pleading[,] [such as through ] . . . affidavits submitted [that] . . . reveal the existence of factual problems in the assertion of jurisdiction." *Carter v. HealthPort Techs.*, LLC, 822 F.3d 47, 57 (2d Cir. 2016) (internal quotation marks and citations omitted).

populate the username and password. (*Id.* ¶ 6.) Notably, the Coding Error did not result from a sophisticated attack perpetrated by cyber criminals or state sponsored hackers. (Compl. ¶ 3.)

Immediately upon learning of the Coding Error, Defendants updated the affected code to eliminate the error. (*Id.* ¶ 24; Hall Decl. ¶ 12.) Defendants also implemented a process that required all potentially affected customers—whether or not they were actually affected—to change their password. (Hall Decl. ¶ 13.) Defendants also began working with the businesses to which the query strings may have been visible to purge the information. (*Id.* ¶ 14.) Defendants represent that all of these entities agreed to delete the information, and all subsequently confirmed deletion. (*Id.*)

Defendants also immediately began investigating which customers' usernames and passwords may have been embedded in the query strings due to the Coding Error. (*Id.* ¶ 16.) Defendants represent that they had to parse through millions of website login attempts and, for each login attempt, identify whether the Coding Error had actually occurred during the login attempt and, if so, match the information to a specific customer. (*Id.*) Defendants represent that they identified each of their customers who could have been potentially impacted by the Coding Error. (*Id.* ¶ 17.)

Defendants also began fraud-monitoring efforts to assess threats or risks of fraud specific to the Coding Error, including monitoring the accounts of potentially affected customers for fraudulent, suspicious, or anomalous activity. (*Id.* ¶ 15.)

On June 11, 2021, Defendants sent a letter to those customers whose information had been embedded in the query strings as a result of the Coding Error. (*Id.* ¶ 18.) This letter explained the circumstances of the Coding Error and the remedial steps that Defendants took after discovering it, including (1) updating the code; (2) requiring customers to reset their passwords; (3) confirming that all third parties would delete the information; and (4) monitoring customers' accounts. (*See*

Compl. ¶¶ 1, 12; *see also* Hall Decl. ¶¶ 18, 20, Ex. A (copy of letter sent to Plaintiff).) By their letter, Defendants also offered all affected customers with free credit monitoring and identity theft insurance coverage for two years. (Compl. ¶ 10; Hall Decl. ¶ 19, Ex. A.)

Defendants further represent that, since discovering the Coding Error on April 12, 2021, their internal cyber risk and fraud teams have monitored the accounts of affected customers for any increase in potential fraudulent or other anomalous activity. (Hall Decl. ¶ 21.) Defendants represent to have identified no instances of account takeovers, identity theft, or similar occurrences attributable to the Coding Error. (*Id.* ¶ 22.) Additionally, Defendants represent that they have not identified any increased rates of potentially fraudulent activity or other anomalous events attributable to the Coding Error. (*Id.*)

Nonetheless, Plaintiff claims to have suffered "imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse" as a result of Defendants negligently disclosing his private information through the Coding Error. (Compl. ¶¶ 30, 35.) Plaintiff alleges that he has been "compelled to devote time to deal with the consequences" of the Coding Error, which includes, "time spent verifying the legitimacy of [Defendants' letter], exploring credit monitoring and identify theft protection, self-monitoring his accounts," and changing his passwords and usernames on his accounts, all of which is time he has "lost forever[.]" (*Id.* ¶¶ 31–32.) He also claims to have suffered "actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property" that he entrusted to Defendants for purposes of facilitating his accounts with them. (*Id.* ¶ 33.)

## II. Procedural Background

On August 13, 2021, Plaintiff filed his operative class action Complaint (Compl., ECF No. 5.) On September 17, 2021, Defendants filed a letter seeking leave to file a motion to dismiss, which the Court subsequently granted and for which it set a briefing schedule. (*See* ECF Nos. 10

& 15.) On December 9, 2021, the parties filed their respective briefing on the instant motion: Defendants their notice of motion (ECF No. 18), memorandum in support ("Motion," ECF No. 19), declaration with supporting exhibits ("Hall Declaration," ECF No. 20), reply ("Reply," ECF No. 23), and supplementary declaration ("Hall Supplementary Declaration," ECF No. 24); and Plaintiff his response in opposition ("Response in Opposition," ECF No. 21) and declaration with supporting exhibits ("De Medicis Declaration," ECF No. 22.)

## LEGAL STANDARD

### I. Federal Rule of Civil Procedure 12(b)(1)

A case is properly dismissed for lack of subject matter jurisdiction under Rule 12(b)(1) when the district court lacks the statutory or constitutional power to adjudicate it. *Makarova v. United States,* 201 F.3d 110, 113 (2d Cir. 2000). The plaintiff bears the burden of establishing the existence of federal jurisdiction. *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560–61 (1992). But "[f]or purposes of ruling on a motion to dismiss for want of standing, both the trial and reviewing courts must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party." *Warth v. Seldin*, 422 U.S. 490, 501 (1975).

"A Rule 12(b)(1) motion challenging subject matter jurisdiction may be either facial or fact-based." *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 56 (2d Cir. 2016). "When the Rule 12(b)(1) motion is facial, *i.e.*, based solely on the allegations of the complaint or the complaint and exhibits attached to it, the plaintiff has no evidentiary burden." *Id.* (citations omitted). "The task of the district court is to determine whether the [complaint and exhibits attached to it] 'allege facts that affirmatively and plausibly suggest that [the plaintiff] has standing to sue." *Id.* (citations omitted). "For purposes of ruling on a motion to dismiss for want of standing, both the trial and reviewing courts must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party." *Warth v. Seldin*, 422 U.S. 490, 501 (1975).

"Alternatively, a defendant is permitted to make a fact-based Rule 12(b)(1) motion, proffering evidence beyond the Pleading." *Carter*, 822 F.3d at 57 (citations omitted). "In opposition to such a motion, the plaintiffs will need to come forward with evidence of their own to controvert that presented by the defendant 'if the affidavits submitted on a 12(b)(1) motion . . . reveal the existence of factual problems' in the assertion of jurisdiction." *Id.* (citing *Exchange National Bank of Chicago v. Touche Ross & Co.*, 544 F.2d 1126, 1131 (2d Cir. 1976)). "However, the plaintiffs are entitled to rely on the allegations in the Pleading if the evidence proffered by the defendant is immaterial because it does not contradict plausible allegations that are themselves sufficient to show standing." *Id.* "If the extrinsic evidence presented by the defendant is material and controverted, the district court will need to make findings of fact in aid of its decision as to standing." *Id.* Indeed, courts "must" consult factual submissions "if resolution of a proffered factual issue may result in the dismissal of the complaint for want of jurisdiction." *Robinson v. Gov't of Malaysia,* 269 F.3d 133, 140 n. 6 (2d Cir. 2001).

**II. Federal Rule of Civil Procedure 12(b)(6)**

In deciding a motion to dismiss under Rule 12(b)(6), the Court must accept all factual allegations in the complaint as true and draw all reasonable inferences in the plaintiff's favor. *Freidus v. Barclays Bank PLC,* 734 F.3d 132, 137 (2d Cir. 2013). To survive a motion to dismiss, a complaint must contain "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Mere "labels and conclusions" or "formulaic recitation[s] of the elements of a cause of action will not do"; rather, the complaint's "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Twombly,* 550 U.S. at 555. In applying these principles, the Court may consider facts alleged in the complaint and documents attached to it or incorporated by reference. *Chambers v. Time Warner, Inc.,* 282

F.3d 147, 152–53 (2d Cir. 2002) (internal quotation marks and citation omitted).

**DISCUSSION**

Plaintiff asserts claims against Defendants for (1) negligence, (2) negligence *per se*, (3) breach of implied contract, (4) violations of the Virginia Personal Information Breach Notification Act, and (5) injunctive/declaratory relief under the Declaratory Judgment Act. (*See* Compl. ¶¶ 60–99.) Defendants seek to dismiss Plaintiff's Complaint for lack of standing—that is, for Plaintiff's failure to allege an injury in fact—and in the alternative, for failure to state a claim. (*See* Mot. at 14–32.)

Accordingly, the Court must first address Defendants' challenge to subject matter jurisdiction and will only analyze Defendants' remaining arguments if the Court has subject matter jurisdiction over this case. *See Brokamp v. James*, --- F. Supp. 3d ---, No. 1:21-CV-00389 (DNH) (ATB), 2021 WL 5444277, at *2 (N.D.N.Y. Nov. 22, 2021) ("Subject matter jurisdiction is a threshold issue and, thus, when a party moves to dismiss under both Rules 12(b)(1) and 12(b)(6), the motion court must address the 12(b)(1) motion first." (citations omitted).)

**I. Standing**

Defendants contend that Plaintiff fails to allege either (a) a requisite concrete, particularized, present injury in fact, or (b) a substantial risk of future injury, to sufficiently establish the injury requirement for purposes of Article III standing. (*See* Mot. at 14–21.)

"Standing is a federal jurisdictional question 'determining the power of the court to entertain the suit.'" *Carver v. City of New York*, 621 F.3d 221, 225 (2d Cir. 2010) (quoting *Warth v. Seldin*, 422 U.S. 490, 498 (1975)). There are three Article III standing requirements: (1) the plaintiff must have "suffered an injury-in-fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *John v. Whole Foods Market Group, Inc.*, 858 F.3d 732, 736 (2d Cir. 2017) (citing *Lujan v. Defenders of*

*Wildlife*, 504 U.S. 555, 560–61 (1992)). "Each element of standing 'must be supported . . . with the manner and degree of evidence required at the successive stages of the litigation,' and at the pleading stage, 'general factual allegation of injury resulting from the defendant's conduct may suffice.'" *John*, 858 F.3d at 736 (quoting *Lujan*, 504 U.S. at 561).

*A. Injury*

An injury in fact "'consists of an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.'" *John*, 858 F.3d at 736 (quoting *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547–48 (2016)). To satisfy the "injury in fact" element in cases involving allegations of "unauthorized exposure of th[e] plaintiff's data," the complaint must establish either a present injury or a future injury due to the alleged exposure. *See McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 300–01 (2d Cir. 2021). A future injury may satisfy the "injury in fact" requirement "only if the threatened injury is certainly impending, or if there is a substantial risk that the harm will occur." *Id.*

1. Concrete, Particularized Present Injury in Fact

Defendants first argue that Plaintiff fails to allege any concrete, particularized present injury in fact because he does not allege that there was any actual misuse of his personal information. (*See* Mot. at 15–17.) Defendants further argue that Plaintiff's other allegations regarding the diminution of value of his private information and the alleged three attempts to access his email account since the Coding Error fail to sufficiently establish an actual or present injury as a matter of law. (*Id.*) After due consideration, the Court agrees.

When construing the Complaint in his favor, the Court construes Plaintiff to allege that he suffered the following present injuries: (1) the "time spent" monitoring his accounts, "exploring credit monitoring and identity theft protection," and changing his passwords and usernames on various online accounts (Compl. ¶¶ 31–32); (2) the "diminution in the value" of Plaintiff's private

information (*id.* ¶ 33); and (3) the "three attempts by hacker[s] to reset the password of his email account without his knowledge or permission" (*id.* ¶ 51).

*a) Time Spent on Mitigating Risks*

With respect to the first alleged present injury, however, only where plaintiffs have "shown a substantial risk of future identity theft or fraud [will] any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact." *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 303 (2d Cir. 2021). That is because plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id*. (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013)). In other words, as a matter of law, Plaintiff's allegations about the "time spent" monitoring his accounts, "exploring credit monitoring and identity theft protection," and changing his passwords and usernames on various online accounts, cannot constitute a present injury in fact in the absence of a substantial risk of future identity theft. As such, the Court will evaluate the sufficiency of this alleged injury after evaluating whether Plaintiff sufficiently alleged a substantial risk of future injury.

*b) Diminution of Value in Private Information*

With respect to the second alleged injury, the Court is of the view that Plaintiff fails to establish that he suffered an alleged "diminution in the value" of his private information because he fails to allege that there is a market for such information.

"Allegations that a plaintiff's private information has lost value may plead a cognizable economic injury." *Wallace v. Health Quest Sys., Inc.*, 20 CV 545 (VB), 2021 WL 1109727, at *8 (S.D.N.Y. Mar. 23, 2021) (citing *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 995 (N.D. Cal. 2016)). "However, such allegations are actionable *only if* the plaintiff also alleges the

existence of a market for that information and how the value of such information could have decreased due to its disclosure." *Id.* (emphasis added) (citing *Rudolph v. Hudson's Bay Co.*, 2019 WL 2023713, at *8 (S.D.N.Y. May 7, 2019)); *see also Welborn v. IRS*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016) ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value."); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 695 (7th Cir. 2015) (alleged "loss of [plaintiffs'] private information" is an "abstract injury" that cannot "support[] standing," "particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value").

Here, even when drawing all inferences in his favor, nowhere in the Complaint does Plaintiff plausibly allege that the Coding Error caused his private information to lose value. Most notably, Plaintiff alleges that his "private information" that lost value as a result of the Coding Error includes his username and password of his account with Defendants. (*See* Compl. ¶ 19.) Yet, Plaintiff fails to allege what inherent value, if any, usernames and passwords have when compared to, for example, highly sensitive personal identifying information—such as names, birth dates, Social Security numbers, driver license numbers, etc.—which, unlike the former, cannot be easily changed at a moment's notice. *See, e.g.*, *Welborn*, 218 F. Supp. 3d at 78 ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value."); *Remijas*, 794 F.3d at 695 (alleged "loss of [plaintiffs'] private information" is an "abstract injury" that cannot "support[] standing," "particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value"). Put another way, the potential independent economic value of a username and password can instantly vanish upon an owner changing them, which is not the case with highly sensitive personal identifying information.

To be sure, Plaintiff does allege that access to an online account with Defendants through the disclosed usernames and passwords could lead to access to highly sensitive personal identifying information. (*See* Compl. ¶ 28.) However, nowhere does Plaintiff allege that any such access ever in fact occurred with respect to his account or those of Defendants' other customers.

And even when assuming that such usernames and passwords have any independent economic value, Plaintiff still fails to allege any facts indicating how the Coding Error diminished such economic value. Indeed, Plaintiff does not even allege the existence of a market for usernames and passwords; instead, at best, Plaintiff only alleges the existence of a black market for private information generally. (*See* Compl. ¶ 40 ("Legitimate organizations and the criminal underground alike recognize the value of Private Information contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it."). "But [even then,] [P]laintiff[] provide[s] only speculative allegations regarding the value of [his] Private Information on that black market and how [his] Private Information diminished in value." *Wallace*, 2021 WL 1109727, at *8; *cf. In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 16-MD-02752-LHK, 2017 WL 3727318, at *13–*14 (N.D. Cal. Aug. 30, 2017) (allegations that information was "highly valuable to identity thieves" and "hackers have sold this [information]," including specific examples of sales, were sufficient to allege plaintiffs lost the value of their private information).

*c) Attempts to Access Plaintiff's Email Account*

And with respect to the third alleged injury (*i.e.*, the multiple attempts to access his email account), even when construing the Complaint in his favor, Plaintiff still fails to establish that he suffered a concrete, particularized injury because the alleged attempts were all unsuccessful. Namely, even when taking his allegation that "hackers" attempted to access his email account as true, (*see* Compl. ¶ 51), Plaintiff nonetheless implicitly admits that these attempts were all

unsuccessful. *See Transunion LLC v. Ramirez*, 141 S. Ct. 2190, 2214 (2021) ("No concrete harm, no standing."); *Whalen*, 689 F. App'x at 90 (attempted fraud insufficient to constitute injury). And even when assuming that an unsuccessful attempt can constitute concrete harm, the Court agrees with Defendants that Plaintiff insufficiently alleges any plausible link between the Coding Error and these alleged access attempts, particularly because Plaintiff alleges that "hackers" attempted to access his *email account* and not any of the online accounts he has with Defendants. (*See* Mot. at 17.)

In response, Plaintiff submits a declaration in which he states that, sometime after the Coding Error, his username for his email account was similar to that for his online account with Defendants. (De Medicis Decl. ¶ 4, ECF No. 22.) He also asserts that his FanDuel account, a sports betting website, was locked after there were multiple unsuccessful login attempts. (*Id.* ¶ 7.) Plaintiff further asserts that in one instance, he received an email notification of an attempted access to his online account with Defendants. (*Id.* ¶ 6.) Plaintiff lastly claims that Defendants themselves actually later placed his online accounts on hold in another instance, for which he had to spend a substantial amount of time addressing the issue. (*Id.* ¶¶ 9–11.)

But Plaintiff's assertions in his declaration still fail to allege a plausible link between the Coding Error and these alleged attempts. First, Plaintiff's assertions relating to his email account, like his relevant insufficient allegation in the Complaint, at best only establish an alleged implied temporal connection between the Coding Error and the multiple login attempts from other countries: that the unsuccessful attempts occurred about six months after the Coding Error.

"Generally, to prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2012). For example, in *Stollenwerk v. Tri–*

*West Health Care Alliance*, 254 F. App'x 664 (9th Cir. 2007), an unpublished opinion on summary judgment, the Ninth Circuit found that a plaintiff sufficiently showed a causal relationship where "(1) [plaintiff] gave [the defendant] his personal information; (2) the identity fraud incidents began six weeks after the hard drives containing [defendant's] customers' personal information were stolen; and (3) [plaintiff had] previously not suffered any such incidents of identity theft." *Stollenwerk v. Tri–West Health Care Alliance*, 254 F. App'x 664, 667 (9th Cir. 2007). There, the court stated that these three facts, in conjunction with the inference a jury could make that the type of information stolen was the same type of information needed to open the fraudulent accounts, were sufficient to defeat a motion for summary judgment brought on the basis of a failure to establish causation. *Id.* at 667–68. Even with this close connection in time, the court recognized that allegations only of time and sequence are not enough to establish causation: "purely temporal connections are often insufficient to establish causation. . . . [H]owever, proximate cause is supported not only by the temporal[ ] but also by the logical[ ] relationship between the two events." *Id.* at 668 (citation omitted); *accord Resnick*, 693 F.3d at 1326–27.

Additionally, in *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012), while discussing *Stollenwerk*, the Eleventh Circuit implied that the longer the time span between the alleged data breach and the identity theft, the stronger the non-temporal nexus between the two incidents must be for a plaintiff to sufficiently allege causation. *See Resnick*, 693 F.3d at 1327. In fact, in *Resnick*, the Eleventh Circuit found that plaintiffs had sufficiently established a non-temporal nexus despite the fact that the time gaps between the alleged breach and identity thefts were of ten and fourteen months (or "six times greater than the one in *Stollenwerk"*):

> Here, Plaintiffs allege a nexus between the two events that includes more than a coincidence of time and sequence: they allege that the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs' identity. . . . Plaintiffs explicitly make this connection when they allege that Curry's identity

> was stolen by changing her address and that Moore's identity was stolen by opening an E*Trade Financial account in his name because in both of those allegations, Plaintiffs state that the identity thief used Plaintiffs' sensitive information. . . . We understand Plaintiffs to make a similar allegation regarding the bank accounts opened in Curry's name even though they do not plead precisely that Curry's sensitive information was used to open the Bank of America account. The Complaint states that Curry's sensitive information was on the unencrypted stolen laptop . . . , that her identity was stolen, and that the stolen identity was used to open unauthorized accounts . . . . Considering the Complaint as a whole and applying common sense to our understanding of this allegation, we find that Plaintiffs allege that the same sensitive information that was stored on the stolen laptops was used to open the Bank of America account.[] Thus, Plaintiffs' allegations that the data breach caused their identities to be stolen move from the realm of the possible into the plausible. Had Plaintiffs alleged fewer facts, we doubt whether the Complaint could have survived a motion to dismiss. However, Plaintiffs have sufficiently alleged a nexus between the data theft and the identity theft and therefore meet the federal pleading standards.

*Id.*

To that end, when drawing all inferences in his favor, Plaintiff here at best establishes the first two *Stollenwerk* factors: that (1) Defendants possessed the content of Plaintiff's username and password; and (2) the attempts to access his email account occurred about six months after the Coding Error. *See Stollenwerk*, 254 F. App'x at 667. Yet, Plaintiff still fails to establish the third factor—that he did not suffer any attempts to access his email account prior to the Coding Error. Indeed, given that the time gap between the Coding Error and the unsuccessful login attempts here was about six months (or twenty-four weeks, which is four times greater than the one in *Stollenwerk*), Plaintiff's allegations—even when taken as true—are the more inadequate to establish a sufficient non-temporal nexus between the two incidents. *See Resnick*, 693 F.3d at 1327.

And moreover, by the rest of his assertions in his declaration, Plaintiff inappropriately seems to "shore up a deficient complaint through extrinsic documents submitted in opposition to a defendant's motion to dismiss." *Madu, Edozie & Madu, P.C. v. SocketWorks Ltd. Nigeria*, 265

F.R.D. 106, 123 (S.D.N.Y. 2010) (citing *Wright v. Ernst & Young LLP,* 152 F.3d 169, 178 (2d Cir. 1998) (holding that plaintiff could not amend her complaint through a legal memorandum filed in opposition to a motion to dismiss). That is because nowhere in his Complaint does Plaintiff allege that there were other attempts to access any of his other online accounts besides those attempts he alleged with respect to his email account.

It is true that courts must necessarily consider a plaintiff's affidavit and other materials submitted to oppose a defendant's fact-based 12(b)(1) motion. *See Carter*, 822 F.3d at 57. But in order to be considered, the plaintiff's affidavit and materials must "*controvert*" those materials submitted by the defendant that purportedly reveal the existence of a factual problem in the plaintiff's assertion of jurisdiction. *Id.* (emphasis added). Otherwise, courts would be effectively allowing plaintiffs to amend any defective allegations by their motion papers submitted in opposition to a 12(b)(1) motion. Hence, the Court must reject Plaintiff's new allegations in his declaration.

And even if the Court were to consider Plaintiff's new allegations in his declaration, such allegations still fail. First, Plaintiff's allegations related to his FanDuel account suffer from the same deficiencies from which the allegations related to his email account suffer (*i.e.*, failing to establish a plausible causal connection). Second, as Defendants' supplementary declaration shows, the email notification Plaintiff received of an attempted access to his online account with Defendants resulted from failed log-in attempts by financial aggregators[2] that Plaintiff himself

[2] As Defendants explain in their supplementary declaration,

> A "financial aggregator" is a website that links and has access to a customer's account. Typically, "financial aggregators" gain access to an account when the account holder sets up access by providing their . . . username and password [with Defendants] to that company. For example, Intuit, a tax-related financial aggregator, is one of [Defendants'] largest financial aggregators with access to [Defendants'] customers' accounts.

uses to link his other online accounts to the one he has with Defendants. (*See* Hall Suppl. Decl. ¶ 8.) And third, as Defendants' supplementary declaration also shows, Plaintiff temporarily lost access to his online account with Defendants after he commenced the instant action because Defendants instituted a legal preservation hold that is intended to prevent any record purges for purposes of litigation—and not because of "hackers" attempting to login into his account. (*Id.* ¶¶ 3–5.)

In sum, the Court concludes that Plaintiff fails to establish that he suffered a concrete, particularized present injury in fact.

2. Substantial Risk of Future Injury

Next, with respect to an alleged substantial risk of future injury, Defendants argue that Plaintiff's allegations about future injury fail as a matter of law under Second Circuit precedent because (i) the Coding Error was inadvertent and not the result of a targeted attack; (ii) the transmitted information has not been misused; and (iii) the transmitted information was neither sensitive nor high risk. (*See* Mot. at 17–21.) The Court agrees.

In *McMorris v. Carlos Lopez & Associates*, LLC, 995 F.3d 295 (2d Cir. 2021), the Second Circuit held that Article III standing in an "unauthorized data disclosure" action could be based on a "substantial risk of future identity theft or fraud." *Id.* at 300, 303 ("[A] future injury constitutes an Article III injury in fact only 'if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.'" (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014))). From its own and other circuits' precedent, the court drew three factors that "bear on whether the risk of identity theft or fraud is sufficiently 'concrete, particularized, and . . . imminent'" for purposes of Article III standing in data-exposure cases: whether (1) "the plaintiffs'

(Hall Suppl. Decl. ¶ 9.)

data has been exposed as the result of a targeted attempt to obtain that data"; (2) "any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud"; and (3) "the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." *Id.* at 303.

Here, regarding the first—and most important—factor, *see id.* at 301, Plaintiff himself alleges that the Coding Error was "inadvertent" and the result of a "'programming' error in [Defendants'] customer website" rather than a "sophisticated attack perpetrated by cyber criminals or state sponsored hackers." (Compl. ¶¶ 1–3, 12, 63.) "Where plaintiffs fail to present evidence or make any allegations that an unauthorized third party purposefully obtained the plaintiffs' data, courts have regularly held that the risk of future identity theft is too speculative to support Article III standing." *McMorris*, 995 F.3d at 301 (collecting cases). Similarly here, the Court concludes that the first factor weighs against Plaintiff.

Regarding the second factor, even when drawing all inferences in his favor, nowhere in the Complaint does Plaintiff allege that the Coding Error resulted in any actual misuses of his username and password. Indeed, at best, Plaintiff alleges that the alleged misuses here include the multiple log-in attempts to his email account. Yet, as already discussed above, Plaintiff nonetheless fails to sufficiently allege how such login attempts are causally connected to the Coding Error such that they could be considered misuses of his disclosed username and password. And moreover, as the Court already concluded above, Plaintiff also fails to plausibly allege that there was a market for his username and password such that one can reasonably infer that there is a substantial risk of future injury. *See McMorris*, 995 F.3d at 301–02 (plaintiff must "show that at least some part of the compromised dataset has been misused," that "plaintiffs' data is already being misused," or that "the plaintiffs' [information] was for sale on the Dark Web"). As such, the Court concludes that the second factor weighs against Plaintiff.

And finally, regarding the third factor, the private information allegedly disseminated here consists of Plaintiff's username and password of his online account with Defendants. As previously discussed, the dissemination of such information stands in stark contrast to the "dissemination of high-risk information such as Social Security numbers and dates of birth, especially when accompanied by victims' names," which "makes it more likely that those victims will be subject to future identity theft or fraud. " *McMorris*, 995 F.3d at 302. Instead, as alleged, Plaintiff's username and password appears to be less sensitive information "that can be rendered useless to cybercriminals [and] does not pose the same risk of future identity theft or fraud to plaintiffs if exposed." *Id.* (finding ability to cancel credit card meant plaintiff did not "plausibly face a threat of future fraud" and thus lacked Article III standing) (citing *Whalen*, 689 F. App'x at 90)); *see also Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021) (same). Hence, the Court concludes that the third factor weighs against Plaintiff.

Thus, because the three *McNorris* factors weigh against him, the Court concludes that Plaintiff fails to plausibly allege a substantial risk of future injury resulting from the Coding Error. And consequently, in the absence of a substantial risk of future injury, Plaintiff's allegations about the "time spent" monitoring his accounts, "exploring credit monitoring and identity theft protection," and changing his passwords and usernames on various online accounts, cannot constitute a present injury in fact. *See McMorris*, 995 F.3d at 303 (holding that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." (quoting *Clapper*, 568 U.S. at 416)).

Therefore, the Court concludes that Plaintiff fails to establish the injury requirement for Article III standing, and dismiss the Complaint accordingly.

## CONCLUSION

For the foregoing reasons, the Court GRANTS Defendants' motion to dismiss (ECF No. 18), and DISMISSES Plaintiff's Complaint without prejudice. The Clerk of the Court is directed to terminate the motion at ECF No. 18 and this action.

Dated: August 2, 2022
White Plains, NY

SO ORDERED:

NELSON S. ROMÁN
United States District Judge